ENGLISH TRANSLATION OF THE INTERNATIONAL APPLICATION

FOR NATIONAL PHASE SUBMISSION

Description

Arrangement comprising an integrated circuit

The invention relates to an arrangement comprising an integrated circuit and to an integrated circuit comprising function modules, wherein the function modules comprise a central processing unit, by means of which data can be processed and programs can be executed, and a cache memory.

Arrangements comprising integrated circuits of the type described above are found today in almost all articles of daily use comprising integrated electronics. Devices for electronic data processing, communication or for recording data have provisions which restrict the read, write or modification access to the data depending on the type of data processed. This is intended to protect data against public accessibility or manipulation. It is particularly in the field of the future generation of tachographs, the digital tachograph, that protection of recorded data against manipulation is of the highest significance.

Previous manipulation-protected systems with high security requirements normally consist of a number of discrete assemblies to which different functions are allocated, for example a central processing unit, an encryption unit and various memories are in each case normally an independent unit which is connected to the other units. The requirement of having a number of assemblies and assembling them and matching

them to one another is associated with high costs in the series production.

Using the problems and disadvantages of the prior art as a starting point, the invention is based on the object of creating an arrangement of the type initially mentioned which meets the highest requirements for manipulation protection and, at the same time, exhibits suitability for series production at lower costs.

The object according to the invention is achieved by means of an integrated circuit of the type initially mentioned, which comprises an encryption unit as function module by means of which data or program code can be encrypted and decrypted.

Due to the fact that an encryption unit, as function module of the integrated circuit, is an element of this component, the additional provision, installation and matching to surrounding components can be saved in the production and development of an arrangement comprising an integrated circuit according to the invention. The further great advantage obtained synergetically is that the encryption unit can be separated only with difficulty from the integrated circuit, the component of which it is, and attempts at manipulation are therefore condemned to fail.

The manipulation of an integrated circuit according to the invention, particularly the separation of individual function modules, is particularly difficult if the integrated circuit is constructed as a semiconductor chip, particularly if

individual function modules are intermeshed in the manner of a puzzle, in such a way that individual function modules can no longer be recognized discretely. In this connection, particularly complex geometric entanglements can be selected so that the intermixed semiconductor structures can no longer be recognized separately as such by means of an analysis with the intention of manipulation.

Additional protection against manipulation is obtained if the function modules comprise a first memory in which cryptological keys are stored. The integration of such a first memory makes a selective access and selective reading-out of the cryptological key more difficult.

The expenditure for the administration of cryptological keys by the manufacturer of the devices is completely absent, with the additional gain in security if the function modules comprise a random-number generator (RNG) which generates the cryptological keys equally autonomously. These keys can be suitably deposited in the first memory.

As a further function module, a real-time clock can be advantageously incorporated in the integrated circuit, the correct function of which also provides high relevance for protection against manipulation.

So that a manipulation attack is not only impaired but rendered impossible, a security sensor system can be advantageously integrated in the circuit as a function module by means of which at least one operating parameter of the

integrated circuit can be monitored. Suitable operating parameters for monitoring are, for example, the clock frequency of the real-time clock, the system or CPU clock, or an operating temperature, or an operating voltage of the integrated circuit, or the state of a protective layer on the integrated circuit, or a combination of the aforementioned operating parameters. If the integrated circuit is constructed as semiconductor component, the monitoring of the state of a protective layer on the integrated circuit is particularly effective since the protective layer must be destroyed in order to access the structure of the semiconductor chip mechanically. In this connection, it is appropriate if the protective layer is constructed as an active protective layer and is applied directly to the die of the semiconductor chip. In a suitable development, it is provided that the active protective layer consists of at least one elongated electrical line which extends along the surface of the die, particularly in mutually parallel tracks section by section. The monitoring can be, for example, a monitoring of the ohmic resistance of the electrical line, wherein a change in the resistance value, which allows a destruction of the electrical line to be inferred, suitably produces a deletion of the data to be protected. The microcontroller is preferably placed into a protective state, for example reset. In this manner, the "integrated circuit" system according to the invention becomes comparatively failsafe.

The monitoring of the operating parameter is suitably handled in such a manner that at least one limit value is predetermined for the operating parameter to be monitored, the

operating parameter is measured and compared with the limit value and when the result exceeds or drops below the limit value, the content of the first memory is deleted. The limit value must be suitably selected in such a manner that the specifications for normal operation do not lead to an interruption of the operation of the arrangement, for example data are not yet deleted at a temperature of -40°C in the automotive field.

The manageability and security of the integrated circuit according to the invention is additionally increased if it is arranged in a package and has terminal contacts brought out of the package. Accordingly, the package would first have to be opened for the purpose of mechanical manipulation.

A greater integration of the circuit according to the invention can be achieved if individual function modules have an essentially planar extent and are arranged adjacently to one another in the direction of the normal to the surface. Thus, for example, the central processing unit can be arranged stacked with various memories or other function modules.

Attacks which draw conclusions regarding the operating state from the behavior of the supply current of the integrated circuit can be advantageously repelled if the function modules comprise an integrated voltage regulator which regulates the operating voltage and in this manner renders this operating parameter comparatively noisy towards the outside.

The integrated circuit according to the invention develops particular advantages in an arrangement having a second memory which is connected to the integrated circuit according to the invention by means of a data bus and in which second memory data or program code are stored encrypted and which has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner. To protect the entire arrangement against failure of an external voltage supply, it is appropriate if it is connected to a battery so that the voltage supply is maintained when another power supply is lacking. Thus, it is also possible to save costs if the second memory is constructed cost effectively to be volatile and is buffered by means of the battery.

As replacement for or supplement to the second memory, a third memory may be appropriate which is connected to the integrated circuit by means of a data bus and is not constructed to be volatile, particularly constructed as flash memory or ROM, wherein the data or program code are preferably stored encrypted in the third memory.

The security sensor system is particularly advantageously buffered by means of a battery. As an alternative or supplement to this measure, an auxiliary power source integrated in the package, for example a capacitor, can be provided which provides the power in the case of a registered manipulation attempt for deleting the memories, particularly the first memory.

In the text which follows, the invention is described in greater detail for the purpose of illustration by means of a special exemplary embodiment. Apart from the present exemplary embodiment, the expert will obtain numerous other design possibilities from the invention described here. In particular, combinations of features which result from combinations of the claims are also attributable to the invention even if no expressed correspondingly reference is given.

Figure 1 shows a diagrammatic representation of an arrangement according to the invention.

Figure 1 shows an integrated circuit 1 comprising a number of function modules 2, which is connected to external components 3. The integrated circuit has, apart from a central processing unit 4, other function modules 2, namely a cache memory 5, an encryption unit 6, a first memory 7, a real-time clock 8, a random-number generator 80 and a security sensor system 9. In addition, a voltage regulator 10 and an auxiliary power source 12 are integrated components of the integrated circuit 1 constructed as semiconductor chip 13. The central processing unit 4 processes data or executes programs which it reads out of the cache memory 5 by means of a first data bus 15.

The cache memory 5 is connected to the encryption unit 6 by means of a second bus 16. The encryption unit 6 reads the encrypted data or code out of the second or third memory 40, 41 by means of the address data bus 32, decrypts them by means of the cryptographic key 18 stored in the first memory 7 and

writes them into the cache or into other internal registers of the central processing unit 4. The cryptographic keys 18 have previously been generated by the random-number generator 80. For generating the cryptographic keys 18 which are stored in the first memory 7, the random-number generator 80 uses, for example, the starting values from the statistical fluctuations (noise) of internal physical measurement quantities such as chip temperature, supply voltage, clock frequency.

Apart from the operating temperature T, the operating voltage U, the clock frequency f, the security sensor system 9 also monitors the ohmic resistance R of a protective layer 20 which consists of essentially parallel tracks of an electrical line 21 which are directly applied to the die of the semiconductor chip 13. The resistance R measured is permanently compared with a limit value and when the limit value is exceeded, the central processing unit 4 initiates the deletion of the first memory 7, the integrated circuit 1 subsequently being brought into a protective state, for example reset.

The integrated circuit 1 is surrounded by a package 30 which has terminal contacts 31 which are at least partially connected to an address data bus 32. The integrated circuit 1 exchanges data with a second memory 40 and a third memory 41 by means of the address data bus 32. The second memory 40 is constructed as volatile RAM and protected against voltage failure by means of a battery 43, as is the integrated circuit 1. The third memory 41 is constructed to be nonvolatile as a flash memory or ROM. The data stored in the second memory 40 and third memory 41 are encrypted by using the cryptological

key 18 and are encrypted or decrypted by means of the encryption unit 6 with each access.